Techno
Gizmo

PUBLIC KEY ENABLING

What is it?

People preparing for TDYs are now required to use the Defense Travel System online, at their desktop, to process their orders. This Public Key-Enabled system requires a person to use their Common Access Card. DTS is among a growing number of everyday, mission-oriented applications that are taking advantage of the benefits Public Key Infrastructure brings by enabling their applications to use the PKI certificates for access, identity verification, and to protect the information resources.

Why do we need it?

The Air Force is committed to achieving Information Superiority through a highly interconnected, network-centric environment and a key to this is the benefits of PKE to improve security of systems and networks. During the past two years the Air Force's focus has been on converting identification cards to the CAC, and providing the middleware and card readers needed to access and use PKI certificates. Those objectives have been achieved, and the Air Force is now moving to the next frontier, PK-enabling of networks and applications.

PKI provides for interoperable security services including authentication, data integrity, and confidentiality, and supports digital signature, access control, and non-repudiation. Everyone uses their CACs at least once each duty day when entering a base. As the Air Force moves into the use of PKI certificates as part of its net-centric business practices, people will use many tools.

PKE and network enabling

One of the tools for network enabling is Smart Card Logon. Smart card certificate-based logon provides the advantage of allowing users to be authenticated with something they know (Personal Identification Number) and something they have (CAC with DOD PKI certificates). The users are not required to remember their network passwords. The certificate used is currently the e-mail signing certificate on the CAC.

Problems addressed with PKE

As SCL is being implemented by major commands across the Air Force, one particular problem continues to surface, logon failures due to certificate errors. Air Force PKI officials are devising a solution to help users determine CAC readiness for SCL. Until then, CAC holders can help make the implementation go smoother by

- verifying that the e-mail signing certificate was issued after May 18, 2002;
- the e-mail address is correct; and
- that the e-mail signing certificate is set as the default certificate.

Another area being addressed is users forgetting their CAC's PIN and locking the CACs. To address this issue and aid the transition to more usage of the CAC, the Air Force is fielding a CAC PIN Reset capability. The CPR system was developed as an alternative to the Military Personnel Flight for unlocking CACs and providing users with an on-site capability to reset their PINs.

SOURCE: AFCA/WFP Information Protection